NASA Standard Operating Procedure

External System Identification and IT Security Requirements

ITS-SOP-0033
Version: 20070719
Effective Date: 19 July, 2007
Expiration Date: 19 July, 2009
Responsible Office: Chief Information Officer

REVISION RECORD

ITEM NO.	REVISION	DESCRIPTION	DATE
1	V 1.0	Steven Adair: Initial document creation.	03/16/2007

External System Identification and IT Security Requirements

1.0 Introduction

It is critical that all NASA stakeholders understand where their information is processed and stored, whether on NASA IT systems or on systems provided by external organizations. In order to ensure that risks to NASA information are managed appropriately, all information must be categorized correctly and all systems containing NASA information must meet the corresponding IT security requirements.

This document has two primary objectives. The first objective is to define what an external system is within the context of NASA's Information Technology (IT) security program and Federal Information Security Management Act (FISMA) requirements. The second objective is to define a standard operating procedure (SOP) that shall be followed to ensure that external systems are meeting Federal and NASA requirements and are adequately protecting NASA information.

Note that the Office of Management and Budget (OMB) uses the term "contractor system" for FISMA reporting purposes. Because this term is not readily defined by OMB or NIST, and because it does not accurately reflect the nature of these systems as opposed to "Agency systems", NASA uses the term "external system" for this purpose.

2.0 System Identification

Each IT systems used by NASA for storing and processing NASA information has to be identified as one of the following in order to address Federal and NASA IT security requirements:

1. Internal system, a.k.a. NASA system – Requirements for such systems are outside the scope of this SOP.
2. External system that stores or processes NASA information that is critical to the mission or operations of NASA – IT security requirements for such systems are described in section 3.0 of this SOP.

2.1 Is the System Internal or External?

Internal systems, also called NASA systems, generally are covered by system security plans (SSPs) developed by NASA or its contractors and exist for the sole purpose of supporting NASA's mission or operations. These systems often are located on NASA owned/leased facilities, use NASA IP addresses, and/or use NASA DNS entries.

Note: This SOP does not address the requirements for internal systems. Information on requirements for internal systems can be found in ITS-SOP-0030 and ITS-SOP-0031 and at http://insidenasa.nasa.gov/ocio/security/CA.html.

External systems are generally owned by outside agencies, contractors, universities, or other organizations and provide services to other customers besides NASA. These systems are usually not located on NASA owned/lease facilities, may not use NASA IP addresses, or may not use NASA DNS entries.

If there is a question about whether a system containing NASA information is an external or an internal system, the NASA Accountable Official and/or the cognizant Center IT Security Manager (ITSM) (see section 4 of this SOP) should use the following questions and their best judgment to determine how the system should be identified.

- Does the system house and/or process NASA information?
- Is the system already covered by an existing NASA SSP?
- Is the primary purpose of the system to support NASA's mission or operation?
- Does NASA own the hardware and/or software associated with this system?
- Is the system operated (administered) by NASA civil servants or contractors?
- Does the system use NASA Internet protocol (IP) addresses and are the addresses used to access the application or service registered to NASA?
- Does the system use the "nasa.gov" domain name service (DNS) in its hostname?
- Is the system physically located at a NASA Center or NASA owned/leased facility?
- Is the system located at a shared facility that servers non-NASA customers?
- Do other personal, private, commercial, or government entities also use the system?

Figure 1 provides more detail and a flowchart of the analysis that should be performed. Using this process, if the main flow (dark arrows) is followed five or more times, then the system is almost certainly an external system.

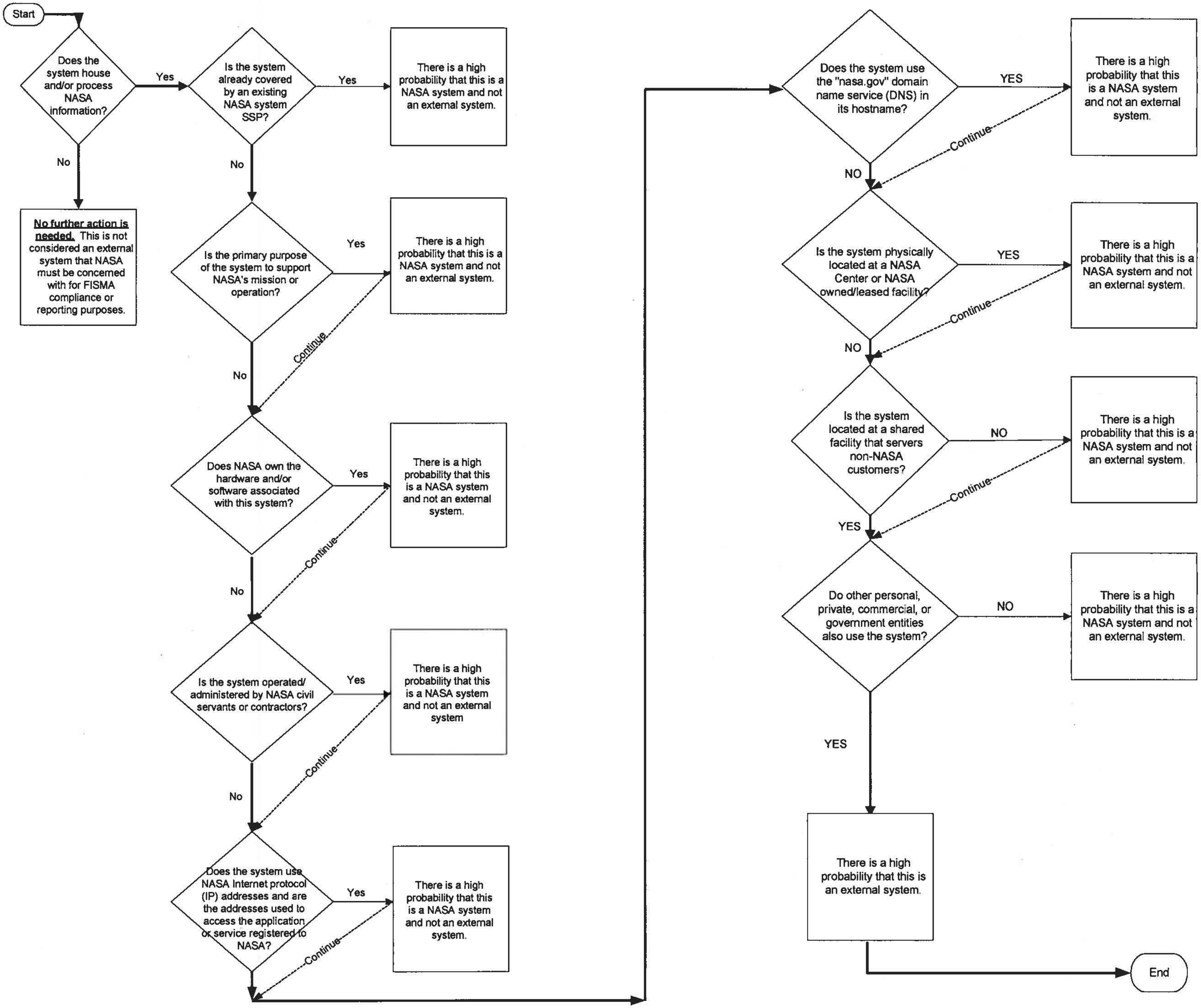
Start
Does the system house and/or process NASA information?
Yes
No
No further action is needed. This is not considered an external system that NASA must be concerned with for FISMA compliance or reporting purposes.
Is the system already covered by an existing NASA system SSP?
Yes
There is a high probability that this is a NASA system and not an external system.
No
Is the primary purpose of the system to support NASA's mission or operation?
Yes
There is a high probability that this is a NASA system and not an external system.
Continue
No
Does NASA own the hardware and/or software associated with this system?
Yes
There is a high probability that this is a NASA system and not an external system.
Continue
No
Is the system operated/ administered by NASA civil servants or contractors?
Yes
There is a high probability that this is a NASA system and not an external system
Continue
No
Does the system use NASA Internet protocol (IP) addresses and are the addresses used to access the application or service registered to NASA?
Yes
There is a high probability that this is a NASA system and not an external system.
Continue
Does the system use the "nasa.gov" domain name service (DNS) in its hostname?
YES
There is a high probability that this is a NASA system and not an external system.
Continue
NO
Is the system physically located at a NASA Center or NASA owned/leased facility?
YES
There is a high probability that this is a NASA system and not an external system.
Continue
NO
Is the system located at a shared facility that servers non-NASA customers?
NO
There is a high probability that this is a NASA system and not an external system.
Continue
YES
Do other personal, private, commercial, or government entities also use the system?
NO
There is a high probability that this is a NASA system and not an external system.
YES
There is a high probability that this is an external system.
End

Figure 1. External/Internal system identification process

2.2 Is the External System Critical to NASA?

Once a system has been identified as an external system, it is necessary to determine whether the system and the NASA information being stored or processed are essential or critical to the mission or operation of the Agency. To do so, the information types that the system houses or processes must be identified and analyzed per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 and a Federal Information Processing Standard (FIPS) 199 information category must be assigned to the system. (NASA ITS-SOP-0019, Procedure for the FIPS 199 Categorization of Systems should be followed.)

If the external system has a FIPS 199 security categorization of

- **Moderate** or **High:** This system must address FISMA compliance and reporting because the system houses or processes information that is essential or critical to the Agency. Such external systems must follow the processes described in section 3 of this SOP;
- **Low:** This system will be considered for FISMA compliance and reporting purposes. The Low categorization should be taken into account when setting priorities in following the processes in section 3.

In the event that there is still ambiguity as to whether or not a system meets the criteria for external systems in sections 2.1 and 2.2, contact the NASA Office of the Chief Information Officer for further guidance.

3.0 Requirements for External Systems

Per OMB memorandum M-06-20, all Federal information systems, including NASA internal systems and external systems, must abide by FISMA requirements. References from M-06-20 follow:

> *1. What systems should be reported under FISMA?*
>
> FISMA applies to information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. All general support systems and applications, whether major or non-major, meeting this definition shall be included in the report. NIST Special Publication 800-37 provides information on establishing information system boundaries which can help you identify your systems.
>
> …
>
> *14. Must all agency systems be tested and evaluated (reviewed) annually?*
>
> Yes, all information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency must be tested at least annually. FISMA (section 3544(b)(5)) requires each agency to perform for all systems

"periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually." This review shall include the testing of management, operational, and technical controls.

It is especially important to note, FIPS 200 (Special Publication 800-53) requires agencies to monitor selected security controls for all systems on a continuous basis. NIST Special Publication 800-37 provides guidance on the continuous monitoring process.

...

26. Must government contractors abide by FISMA requirements?

Yes and each agency must ensure their contractors are doing so. Section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3544(b) requires each agency to provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." This includes services which are either fully or partially provided by another source.

...

31. How deeply into contractor, state, or grantee systems must a FISMA review reach? To the application, to the interface between the application and their network, or into the corporate network/infrastructure?

This question has a two-part answer. First, FISMA's requirements follow agency information into any system which uses it or processes it on behalf of the agency. That is, when the ultimate responsibility and accountability for control of the information continues to reside with the agency, FISMA applies. Second, with respect to system interconnections, as a general rule, OMB assumes agency responsibility and accountability extends to the interface between government systems (or contractor systems performing functions on behalf of the agency) and corporate systems and networks. For example, a corporate network, human resource, or financial management system would not be covered by FISMA requirements, provided the agency has confirmed appropriate security of the interface between them and any system using government information or those operating on behalf of the agency. See also the discussion concerning interconnection agreements and below regarding C&A and accreditation boundaries.

32. Are all IT systems operated by a contractor on behalf of an agency subject to the same type of certification and accreditation process?

Yes, they must be addressed in the same way. As with agency operated systems, the level of effort required for certification and accreditation depends on the impact level of the information contained on each system. Certification and accreditation of a system with an impact level of low will be less rigorous and costly than a system with a higher impact level. More information on system security categorization is available

> in FIPS Pub 199 and NIST Special Publication 800-60 "Guide for Mapping Types of Information and Information Systems to Security Categories".
>
> FISMA is unambiguous regarding the extent to which NIST certification and accreditation and annual IT security self-assessments apply. To the extent that contractor, state, or grantee systems process, store, or house Federal government information (for which the agency continues to be responsible for maintaining control), their security controls must be assessed against the same NIST criteria and standards as if they were a government-owned or operated system. The accreditation boundary for these systems must be carefully mapped to ensure that Federal information: (a) is adequately protected, (b) is segregated from the contractor, state or grantee corporate infrastructure, and (c) there is an interconnection security agreement in place to address connections from the contractor, state or grantee system containing the agency information to systems external to the accreditation boundary.

As clearly stated in the above excerpts from OMB guidance, external systems (as identified in section 2 of this SOP), as well as internal systems, must follow a certification and accreditation (C&A) process that is consistent with the NIST SP 800-37 requirements, and must be reported to OMB for FISMA purposes.

However, there are key differences, from NASA's point of view, between the requirements for internal systems and for external systems:

- For internal systems, NASA is responsible for meeting all requirements, such as completing the C&A process and reporting on key IT security metrics.
- For external systems, NASA is not responsible for actually performing C&A activities. However, a NASA Accountable Official must authorize the system to contain NASA information. Meeting the FISMA requirements and performing the C&A activities are the responsibility of the external system owner, i.e. not NASA program staff or NASA/Center CIO staff. The processes and formats used are required to be consistent with OMB and NIST guidance. NASA is responsible for ensuring that the requirements are met and that NASA information is adequately protected, and for reporting to OMB on the same IT security metrics.
  NASA will accept NIST-based C&A decisions made by other Federal Agencies for external systems that NASA is sharing with the owning Agency. However, annual assessments must still be conducted in accordance with Section 3.1 to ensure that NASA information is being properly protected.

3.1 Meeting the Requirements

An IT security assessment, as outlined in section 3.1.1, needs to be done prior to placing NASA information on an external system and at least annually. The NASA Accountable Official must authorize this information to be placed on the external system per section 3.1.2. Additionally, a quarterly report about each external system is due to the OCIO per section 3.1.3.

3.1.1 Assessment (**Prior to initial authorization and annually**)

The IT security posture of each external systems must be reviewed prior to placing NASA information in the system and annually thereafter. The goal of the assessment is to ensure that NASA information on the external system is adequately protected. There are several ways in which this can be achieved. The Accountable Official is responsible for determining which of the following methods are acceptable:

1. The system has successfully completed the C&A process per NIST SP 800-37 and NASA verifies this by reviewing the system's C&A package and supporting documentation.
2. The system has successfully completed another standardized review and/or certification process, for example, based on the ISO 17799/BS 7799-1:1999 standard, a SAS 70 audit, etc., and NASA verifies this by reviewing the relevant documentation.
3. NASA reviews the management, operational and technical security controls of the system and documents the findings in accordance with NIST SP 800-53A and ITS-SOP-0005.

Any review must be performed by qualified NASA staff or NASA contractor personnel, as designated by the cognizant Center ITSM for the external system. The assessor reports the findings of the IT security assessment using the *Report of External System IT Security Assessment* form found in Appendix A. The cognizant Center ITSM ensures that the report is entered (along with any relevant supporting documentation) in the Center's system security documentation repository.

If security risks were identified during the review, it may be necessary to work with the system owner of the external system to address or mitigate these risks before proceeding.

In some cases, it may not be possible for the external system to meet all the requirements. For example,

- An external system where the external system owner has not met C&A or other requirements and does not intend to do so;
- An existing contract, grant or other agreement that makes it infeasible to meet or enforce the requirements; or
- An external system whose low cost, limited scope or short time of operation does not warrant the expense of C&A, an IT security assessment, or other requirement.

In all cases, it is up to the NASA Accountable Official to decide what risks are acceptable when storing and processing NASA information on an external system, and this decision has to be documented (see section 3.1.2).

There may also be reasons why an IT security assessment cannot be conducted, including

- External system owner concerns, e.g. that the assessment could have an unacceptable impact on the system or that an existing contract or other agreement precludes such an assessment;

- An agreement that the Low categorization of the NASA information or limited scope, monetary value or short time-frame of the system do not warrant an assessment; or
- NASA concerns over resources, logistics, etc. that prevent NASA from performing an assessment.

If an assessment is not conducted, it is again up to the Accountable Official to decide whether to proceed with NASA's use of the external system. The decision must be documented (see section 3.1.2).

NASA may choose not to conduct an assessment if the outcome of the assessment can have no bearing on whether the external system will be used. If NASA is mandated by Federal Law, requirements, or other authoritative guidance to store or process NASA information on a specific external system, the Agency cannot avoid placing information into it regardless of risk. If NASA does not have any influence over the security of an external system and cannot use an alternative solution, the Agency cannot be held responsible for ensuring IT security requirements are met by the system. An example of such as system is the Electronic Questionnaires for Investigations Processing (e-QIP), which NASA is required to use for processing information of at least a Moderate security impact level. In such cases, the use of the external system should be documented in the same way (see section 3.1.2), with an annotation about the limits on NASA's options and control over the security of the external system.

3.1.2 Authorization (**Prior to initial use and at least every three years**)

The findings of the IT security assessment are reported by the cognizant Center ITSM to the Accountable Official using the *Report of External System IT Security Assessment* form found in Appendix A**.** The ITSM should be in a position to explain any identified risks or technical issues to the Accountable Official if necessary.

The Accountable Offical ultimately decides whether NASA information should be (or continue to be) stored and processed on the external system, based on identified or remaining risks and mitigating controls.

The Accountable Offical is also the person to decide whether to accept the risk of not fully understanding the IT security posture of the external system if an IT security assessment was not performed.

In all cases, the Accountable Offical must authorize NASA information to be stored or processed on the external system, using the *Authorization to Process NASA Information on an External System* form in Appendix A, prior to initial use and at least every three years thereafter. The documentation of this authorization must be stored in the relevant Center's system security documentation repository.

3.1.3 Reporting to OCIO (**Quarterly**)

A report on all external systems tracked by each Center ITSM is due to the OCIO on the

15th of February, May, August, and November. Appendix B contains a spreadsheet template that must be used for quarterly reporting to the OCIO. It includes the following information:

- Center (or "NASA")
- System number (per ITS-SOP-0007)
- System Name, Owner, Location
- NASA Accountable Offical and contact info
- Other NASA POC (if applicable) and contact info
- Short description of system and/or NASA data
- FIPS 199 category
- Cognizant Center ITSM
- Date authorization signed
- Date last assessment completed
- Contingency Plan tested in accordance with policy (Y/N)[1]
- Comments

4.0 Roles and Responsibilities

Many of the roles and responsibilities defined in section 2.2 of NIST SP 800-37 also apply to external systems. However, it should be noted that many of these roles, such as the System Owner and Authorizing Official, are not performed by NASA personnel. These roles and responsibilities exist within the organization that owns the system.

Other roles and responsibilities are defined specifically for NASA in this SOP and are described below.

4.1 Cognizant IT Security Manager

One Center ITSM is assigned IT security management and tracking responsibility for each external system. This can be the ITSM at the Center where the external system Accountable Offical resides, where the external system is managed, where the relevant NASA information is generated, or as assigned by the NASA OCIO.

For each external system, the cognizant ITSM is responsible for

- Working with the NASA information owner or Accountable Offical to determine

[1] OMB requires agencies to report whether each system's contingency plan has been tested in accordance with policy. Status of external system contingency plan testing should be verified as follows:

- If the system is in compliance with NIST SP 800-37 (i.e. C&A) requirements, per the NASA IT security assessment, this implies that the contingency plan is being tested in accordance with policy.
- If the system satisfies the security requirements of this SOP under another process, NASA's IT security assessment should include a check whether the system's contingency plan has been tested in accordance with policies relevant to the system or the system owner.
- If NASA is unable to or chooses not to conduct an IT security assessment, NASA should nevertheless ask the system owner whether the system's contingency plan has been tested in accordance with policies relevant to the system.

whether the system is an internal system, an external system, or other (i.e. a system for which NASA is not responsible for compliance or reporting of IT security requirements);

- Conducting or causing to be conducted initial and annual IT security assessments, as applicable;
- Ensuring that an IT security assessment report is prepared as a result of the assessment;
- Ensuring that the results of the IT security assessment are available to the Accountable Offical and that a decision is made and documented on whether any identified risks to NASA information are acceptable and whether NASA information may be (or may continue to be) stored and/or processed on the external system;
- Ensuring that documentation related to IT security of the external system, including system summary information, the report of the IT security assessment, and the *Authorization to Process NASA Information on an External System* are included in the appropriate system security documentation repository; and
- Reporting quarterly to the NASA OCIO on the IT security status of the external system.

4.2 Accountable Official

The role of an Accountable Offical for an external system is somewhat analogous to an Authorizing Official (as defined in NPR 2810) for internal systems. The Accountable Offical is the NASA official who owns or is responsible for the NASA information being stored or processed on the external system. For external systems provided through a contract, this may be the Contracting Officer Technical Representative (COTR). This person is ultimately accountable for the NASA information on the system.

For each external system, the Accountable Offical is responsible for

- Working with the cognizant Center ITSM to determine whether the system is an internal system, an external system, or other (i.e. a system for which NASA is not responsible for compliance or reporting of IT security requirements);
- Working with the cognizant Center ITSM to ensure that an initial and annual IT security assessment is conducted, as applicable;
- Reviewing the results of the IT security assessment;
- Deciding whether or not any identified risks to NASA information are acceptable and whether NASA information may be (or may continue to be) stored and/or processed on the external system. This decision must be documented using the *Authorization to Process NASA Information on an External System*;
- If a decision is made not to store and/or process NASA information on the external system, ensuring that the relevant NASA information is removed from the external system; and
- Working with the cognizant Center ITSM to ensure that documentation related to IT security of the external system, including system summary information, the *Report of External System IT Security Assessment*, and the *Authorization to Process NASA Information on an External System* are included in NASA's system security documentation repository.

4.3 NASA OCIO

For external systems, the NASA OCIO is responsible for

- Developing relevant policies, procedures and guidance, including updates to this SOP in response to changing OMB requirements or other issues;
- Ensuring that the NASA system security documentation repository supports the requirements related to external systems;
- Tracking the IT security status of all external systems; and
- Reporting quarterly to OMB on the IT security status of external systems as required under FISMA.

Signature

Robert Binkley

Robert Binkley
Deputy Chief Information Officer
for IT Security (Acting)

7-20-2007
Date

Appendix A: Forms

Report of External System IT Security Assessment

System (name, plan number per ITS-SOP-0007):	FIPS 199 Security Impact Level: □ High □ Moderate □ Low
Responsible Organization(s)/Center(s):	
Reviewed Security Documentation (SSP, Accreditation Letter, etc.):	
Notable Risks or Exceptions:	
I have assessed the IT security of this external system in accordance with ITS-SOP-0033. As a result of this assessment is my recommendation that NASA information □ should be placed on this system. □ should **NOT** be placed on this system.	
Assessor (name, title, org.):	Contact Information Phone: E-Mail: Fax:
Assessor Signature:	Date:

Authorization to Store/Process NASA Information on an External System

System (name, plan number per ITS-SOP-0007):	FIPS 199 Security Impact Level: □ High □ Moderate □ Low
Responsible Organization(s)/Center(s):	
I hereby authorize the use of this external system for storing and/or processing NASA information, for a period not to exceed 36 months or the occurrence of a significant change, whichever comes first. **This external system has met the IT security requirements defined in NASA ITS-SOP-0033 and any remaining risks are at an acceptable level to adequately assure the IT security of the NASA information being stored and/or processed.**	
NASA Accountable Official (name, title, org.):	Contact Information Phone: E-Mail: Fax:
NASA Accountable Official Signature:	Date:

Appendix B: NASA External Systems Reporting Template

Center (or "NASA")	System number (per ITS-SOP-0007)	System Name, Owner, Location	NASA Accountable Offical and contact info	Other NASA POC (if applicable) and contact info	Short description of system and/or NASA data	FIPS 199 category	Cognizant Center ITSM	Date authorization signed	Date last assessment completed	Contingency Plan tested in accordance with policy (Y/N)	Comments